

REMARKS

Claims 1-84 are pending in the present application. By this Response, claims 45, 48, 52, 54, 73, and 75 are amended for proper dependency. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 103, Alleged Obviousness, Claims 1-84

The Office Action rejects claims 1-84 under 35 U.S.C. § 103(a) as being unpatentable over http://www.verisign.com/support/tlc/class3_install_docs/netcape/v00g.html ("VeriSign") and <http://www-2.cs.cmu.edu/~dmaltz/main-report/node7.html#SECTION00420000000000000000> ("Maltz"). This rejection is respectfully traversed.

As to claims 1, 22, 43, and 64, the Office Action states:

Regarding claim 1, Verisign teaches "A method in a data processing system for an organization to provide anonymity to a user, the method comprising the data processing system implemented steps of: receiving a request from the user for an anonymous identity; generating the anonymous identity for the user, wherein the anonymous identity includes contact information for the organization; associating the anonymous identity with the user, wherein the user uses the anonymous identity to provide information on a network data processing system; receiving a contact directed to the anonymous identity; and...(section "Activating SSL encryption", i.e. selecting alias for the key-pair file)." These passages of Verisign do not teach "selectively forwarding the contact to the user based on a policy" in the sense of the claim.

Matz teaches "selectively forwarding the contact to the user based on a policy (the second paragraph, i.e. user-profile based or rule based filters) for the motivation of having select for a user (the first paragraph).

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine Verisign and Matz for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Office Action dated December 21, 2004, pages 2-3.

Claim 1, which is representative of the other rejected independent claims 12, 14 and 25 with regard to similarly recited subject matter, reads as follows:

1. A method in a data processing system for an organization to provide anonymity to a user, the method comprising the data processing system implemented steps of:
 - receiving a request from the user for an anonymous identity;
 - generating the anonymous identity for the user, wherein the anonymous identity includes contact information for the organization;
 - associating the anonymous identity with the user, wherein the user uses the anonymous identity to provide information on a network data processing system;
 - receiving a contact directed to the anonymous identity; and
 - selectively forwarding the contact to the user based on a policy.(emphasis added)

VeriSign and Maltz, taken alone or in combination, fail to teach or suggest receiving a request from the user for an anonymous identity; generating the anonymous identity for the user, wherein the anonymous identity includes contact information for the organization; associating the anonymous identity with the user, wherein the user uses the anonymous identity to provide information on a network data processing system; receiving a contact directed to the anonymous identity; and selectively forwarding the contact to the user based on a policy.

VeriSign is directed to installing a Secure Site Server ID and Commerce Site Server ID on a Netscape Enterprise Server. The section referred to by the Office Action as teaching or suggesting the above emphasized features teaches configuring a server to use Secure Sockets Layer (SSL) protocol on a server. More specifically, the section cited by the Office Action teaches activating SSL encryption on a server. In order to activate SSL encryption for an administration server, an administrator chooses Admin Preferences|Encryption On/Off in the Server Manager. The Encryption On/Off form appears. The administrator checks the On radio button. Then the administrator chooses the alias for the key-pair file and certificate file that you want to use and was generated earlier. The administrator must know the password for the key-pair file referenced by this alias. The password must be entered before starting or stopping a server that uses SSL encryption. The administrator then sets any desired security preferences, stops the server, and then restarts it from the command-line or NT control panel. The administrator is prompted to enter the password for the key-pair alias that was set up by the administrator during configuration.

There is nothing in this section, or any other section of VeriSign, that teaches or suggests receiving a request from a user for an anonymous identity. VeriSign teaches configuring a server with an alias. An alias is an alternative name for an object, such as a variable, file, or device, more particularly the Netscape Enterprise Server that VeriSign teaches configuring. An administrator entering an alternative name for a server, an alias, as taught by VeriSign is not equivalent to receiving a request from a user for an anonymous identity. Furthermore, VeriSign does not teach or suggest generating the anonymous identity for the user, wherein the anonymous identity includes contact information for the organization. In fact, only the administrator who is configuring the server generates the alias. VeriSign merely teaches storing the alias as an alternative name for the server and does not teach generating an anonymous identity for a user.

Additionally, VeriSign does not teach associating the anonymous identity with the user, wherein the user uses the anonymous identity to provide information on a network data processing system. VeriSign teaches associating an alias with the server, not a user. Furthermore, though VeriSign's configured server may receive a contact from a user directed to the server alias, this receipt is not equivalent to the receipt of a contact directed to the anonymous identity of a user. Still further, VeriSign's contact is held at the server as that is the alias that is used to contact the server, which is not equivalent to selectively forwarding the contact to the user based on a policy as in the presently claimed invention. The Office Action acknowledges that VeriSign does not teach this feature, but alleges that this feature is taught by Maltz. Maltz is directed to selecting articles for a user to view by determining the value of the information contained in the article to the user. Thus, Maltz filters article information to determine if information in the article is similar to information that is specified in a user's profile. If the information is similar, then Maltz sends the information to the user. Maltz does not teach receiving a contact directed to the anonymous identity of a user and selectively forwarding the contact to the user based on a policy.

Furthermore, there is not so much as a suggestion in either reference to modify the references to include such features. That is, there is no teaching or suggestion in VeriSign or Maltz that a problem exists for which receiving a request from the user for an anonymous identity; generating the anonymous identity for the user, wherein the

anonymous identity includes contact information for the organization; associating the anonymous identity with the user, wherein the user uses the anonymous identity to provide information on a network data processing system; receiving a contact directed to the anonymous identity; and selectively forwarding the contact to the user based on a policy, is a solution. The VeriSign and Maltz, either alone or in combination, do not teach or suggest any of the above described features. Neither of the references even recognizes a need to provide the features as recited in claim 1.

Moreover, neither reference teaches or suggests the desirability of incorporating the subject matter of the other reference. That is, there is no motivation offered in either reference for the alleged combination. As discussed above, neither reference receives a request from the user for an anonymous identity; generate the anonymous identity for the user, wherein the anonymous identity includes contact information for the organization; associate the anonymous identity with the user, wherein the user uses the anonymous identity to provide information on a network data processing system; receive a contact directed to the anonymous identity; and selectively forward the contact to the user based on a policy. Neither of the references teaches or suggests an anonymous identity for a user or contact that is directed to an anonymous identity of a user. Thus, the only teaching or suggestion to even attempt the alleged combination is based on a prior knowledge of Applicants' claimed invention thereby constituting impermissible hindsight reconstruction using Applicants' own disclosure as a guide.

One of ordinary skill in the art, being presented only with VeriSign and Maltz, and without having a prior knowledge of Applicants' claimed invention, would not have found it obvious to combine and modify VeriSign and Maltz to arrive at Applicants' claimed invention. To the contrary, even if one were somehow motivated to combine VeriSign and Maltz, and it were somehow possible to combine the systems, the result would not be the invention, as recited in claim 1; the result would be simply configuring a Netscape Enterprise Server to user SSL encryption and filtering articles based on a user profile. The resulting system still would not perform the features recited in claim 1.

Independent claims 14, 35, 56 and 77 recite similar features in their respective claim terminology. Claims 14, 35, 56 and 77 recite "receiving a contact, wherein the contact includes an identification of an entity; comparing the identification of an entity in

the contact to a database of aliases; and responsive to identifying the user, selectively forwarding the contact to the user based on a policy.” Only the server is identified by the alias in the VeriSign reference. VeriSign does not identify a user either directly or through an alias.

In view of the above, Applicants respectfully submit that the VeriSign and Maltz, taken alone or in combination, fail to teach or suggest the features of claims 1, 14, 22, 35, 43, 56, 64, and 77. At least by virtue of their dependency on claims , 14, 22, 35, 43, 56, 64, and 77, the features of dependent claims 2-13, 15-21, 23-34, 36-42, 44-55, 57-63, 65-76, and 78-84 are not taught or suggested in the VeriSign and Maltz, whether taken individually or in combination. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-84 under 35 U.S.C. § 103(a).

As to claims 2, 3, 23, 24, 44, 45, 65, and 66, Applicants respectfully submit that, while such particular features may be well known in the art, VeriSign and Maltz, taken alone or in combination, fail to teach or suggest a Web based system or a system which provides billing. Thus, one of ordinary skill in the art would not find it obvious to combine these well known teaching with VeriSign and Maltz, either alone or in combination.

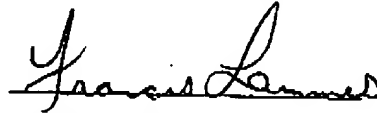
As to claims 4-13, 15-21, 25-34, 36-42, 46-55, 57-63, 67-76, and 78-84, the Office Action does not establish a prima facie case of obviousness with regards to these claims, because the Office Action does not show that VeriSign and Maltz, either alone or in combination, teaches or suggests receiving a request from the user for an anonymous identity; generating the anonymous identity for the user, wherein the anonymous identity includes contact information for the organization; associating the anonymous identity with the user, wherein the user uses the anonymous identify to provide information on a network data processing system; receiving a contact directed to the anonymous identity; and selectively forwarding the contact to the user based on a policy.

II. Conclusion

It is respectfully urged that the subject application is patentable over the prior art of record and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: March 21, 2005

Respectfully submitted,



Francis Lammes
Reg. No. 55,353
Yec & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Agent for Applicants